



AF #2131

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Docket No: Q57604

Toru SUMINO

Appln. No.: 09/487,726

Group Art Unit: 2131

Confirmation No.: 3499

Examiner: Kaveh Abrishamkar

Filed: January 19, 2000

For: INDIVIDUAL AUTHENTICATION SYSTEM PERFORMING AUTHENTICATION IN
MULTIPLE STEPS

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents

P.O. Box 1450

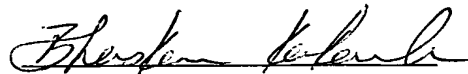
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief. A check for the statutory fee of \$500.00 is attached. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account. A duplicate copy of this paper is attached.

Respectfully submitted,

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860


Bhaskar Kakarla
Registration No. 54,627

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: January 24, 2005



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Docket No: Q57604

Toru SUMINO

Appln. No.: 09/487,726

Group Art Unit: 2131

Confirmation No.: 3499

Examiner: Kaveh Abrishamkar

Filed: January 19, 2000

For: **INDIVIDUAL AUTHENTICATION SYSTEM PERFORMING AUTHENTICATION
IN MULTIPLE STEPS**

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the
following:

TABLE OF CONTENTS

I.	REAL PARTY IN INTEREST.....	3
II.	RELATED APPEALS AND INTERFERENCES	4
III.	STATUS OF CLAIMS	5
IV.	STATUS OF AMENDMENTS.....	6
V.	SUMMARY OF THE CLAIMED SUBJECT MATTER	7
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	9
VII.	ARGUMENT.....	10
	CLAIMS APPENDIX	17

Appeal Brief
USSN 08/487,726

Attorney docket: Q57604
Art Unit 2131

EVIDENCE APPENDIX:	19
RELATED PROCEEDINGS APPENDIX.....	20

I. REAL PARTY IN INTEREST

The real party in interest is NEC Corporation, the assignee of the present application.

The assignment was recorded on May 25, 2000, at reel 010811, frame 0267.

II. RELATED APPEALS AND INTERFERENCES

Appellant, Appellant's legal representatives, and the assignee in this application are not aware of any other pending appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

Claims 1, 3, 5 and 7-10 are all of the claims currently pending in the present application, and currently each of these claims stand rejected by the Examiner in the Final Office Action (paper no. 11) dated May 26, 2004, which is the subject of this appeal.

Claims 2, 4 and 6 have been canceled during prosecution of the present application.

IV. STATUS OF AMENDMENTS

There are no outstanding, non-entered amendments of the claims.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This invention relates to an individual authenticating system for authenticating a user of a data processing device (Specification at page 2, lines 11-13). One object of the invention is to provide a system where the data processing device can be used and managed with a higher security than conventional systems (Specification at page 2, lines 12-13).

One embodiment of the invention (claim 1) provides an individual authentication system for authenticating the user of a data processing device (2) storing a password (16) (Fig. 1), that comprises an individual authentication card (1) for storing biological information (12) and a password (13) for identifying a registered user (Specification at page 4, lines 18-20, Fig. 1). The individual authentication system also comprises: a card reader (23) for reading out the biological information (12) and the password (13) stored in the card (1) (Specification at page 4, line 24 to page 5, line 1); a biological information input device (22) for inputting biological information (15) from a user (Specification at page 6, lines 11-13, Fig. 1); and means (24) for respectively collating the biological information (12) and the password (13) read from the card reader (23) with the biological information (15) from the biological information input device (22) and the password (16) stored in the data processing device (2) (Specification at page 5, lines 2-5).

A non-limiting example of the structure for the means (24) for respectively collating the password and biological information described above may be found in the Specification at page 5, lines 2-6 and at page 6, lines 20-22 and in Fig. 2, element 24. These sections describe a built-in collating unit (24) in computer (2), which is illustrated in Fig. 2.

The data processing device (2) also has an identification number input device (2) by which the user inputs an identification number (14) (Specification at page 5, lines 20-24).

The card (1) stores an identification number (11) for identifying the registered user, and the card (1) has a function of collating the stored identification number (11) with the

identification number (14) transmitted by the identification number input device (21)

(Specification at page 5, line 24 to page 6, line 1).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1, 3 and 7-10 are unpatentable under 35 U.S.C. § 103(a) in view of Moussa *et al.* (USP 6,035,406) [“Moussa”], Dunn *et al.* (USP 5,987,155) [“Dunn”] and Teicher *et al.* (USP 6,257,486) [“Teicher”].

2. Whether claim 5 is unpatentable under 35 U.S.C. § 103(a) in view of Moussa, Dunn, Teicher and Pearson *et al.* (USP 5,991,408) [“Pearson”].

VII. ARGUMENT

Claims 1, 3 and 7-10:

Claim 1 recites an individual authentication system that comprises “an individual authentication card ... [that] has a function of collating the stored identification number with the identification number transmitted by the identification number input device.” The Examiner concedes that this feature is not explicitly disclosed by Moussa but applies Teicher to allegedly cure the deficiency.

In order to establish a *prima facie* case of obviousness the prior art must provide some suggestion or motivation for combining the references. See MPEP 2143.

Appellant submits that the prior art references teach away from one another, therefore, the Examiner has not established a *prima facie* case of obviousness because there is no suggestion or motivation to combine the references.

For Example, Moussa discloses the following:

Electronic security systems which require a physical token may operate by using a challenge and response system, in which the system issues an electronic challenge to the physical token and in which the user interacts with the physical token to obtain an electronic response. If the response is one which the system associates with the challenge as proper, the physical token is recognized and the security system is able to authenticate the user, at least using the physical factor.

A first problem which has arisen in the art is that such **physical tokens [in which the user interacts with the physical token]** are thus required to be "active," that is that they require electrical power to operate and **therefore have a limited operational lifetime.**

A second problem which has arisen in the art is that known security systems which require such physical tokens operate by first authenticating the user using secret information (such as requiring the user to log in using a password), then

execute an application program for security authentication of the physical token. Similarly, known security systems which require biometric information operate by first authenticating the user using secret information, then execute an application program for security authentication of the biometric information. **Security systems which allow users to execute application programs before they have been fully authenticated are considered less secure than those which do not.**

A **third problem** which has arisen in the art is that known security systems which require such physical tokens require the user to enter the secret information (such as a password or PIN) to the physical token for the challenge and response. This **provides an additional source for authentication error or for exposure of the user's secret information, neither of which would be desirable.**

Accordingly, **it would be desirable** to provide a method and system for providing authentication using two or more factors **without allowing the user to execute any application programs before authentication for all factors is complete.** It would also be **desirable** to provide a method and system for providing electronic authentication **using a physical token which does not require electrical power to operate.** It would also be desirable to provide a method and system for providing electronic authentication **using a physical token which does not require the user to enter data or otherwise interact with the physical token.** These advantages are achieved in an embodiment of the invention in which the physical token includes a **passive storage device** and a **login service obtains password information from the storage device**, so as to **simultaneously authenticate the user with both a password and the physical token itself.**

Col. 1, line 20 to col. 2, line 2. (Bold and underline added for emphasis).

To summarize the disclosure of Moussa given above, Moussa identifies three problems associated with active physical tokens: 1) limited operational lifetime, 2) execution of a program to validate the physical token without fully validating the user and 3) provides an addition source of errors and an opportunity to acquire user's secret information. To solve these problems, Moussa disclose a principle of operation which uses a passive (un-powered)

physical token and a login service that provides simultaneous authentication of the user by using a password and the physical token.

The simultaneous authentication is accomplished by the login service 140, which intercepts attempts by the user to log into the processor 110 by interacting with the physical token 131 and the operating system 150 (See col. 3, lines 20-23). The login service 140 authenticates a user by verifying a password entered by the user with one stored on the physical token 131, and the login service 140 also verifies fingerprint data D stored on the physical token with fingerprint data F stored in a database 141 (col. 4, lines 1-10, and col. 4, lines 56-58, Fig. 1).

Since the disclosed principle of operation in Moussa teaches away from the conventional “challenge and response” method where a user interacts with a physical token by inputting a PIN or password in response to a request, additional errors and possible security problems associated with the user’s interaction with the physical token is eliminated (See col. 1, lines 20-53).

For at least the reasons given above, Appellant submits that Moussa clearly teaches away from the use of an active physical tokens that require the user to enter data on the physical tokens.

In direct contrast to Moussa, Teicher teaches authenticating a user by entering a PIN directly onto a smart card (physical token) and also teaches the use of a powered card (See Abstract, Fig. 11). In addition, Teicher teaches away from authenticating a PIN outside the smart card (such as with computers, see Figs. 9A and 9B) because such a system is less secure than interacting with the smart card (see Abstract). For example, Teicher teaches that using a computer presents security hazards because electrical connections from keyboards

can be tapped. In addition, computer hardware is not designed to resist tampering and much of the operating system takes place in software that is readily accessible to an attacker (col. 10, lines 1-8).

Thus, Appellants submit that Teicher clearly teaches away from the login service of Moussa, which would authenticate password and fingerprint data by running a program that is outside the physical token.

Dunn discloses a biometric input device such as a fingerprint device (col. 1, lines 57-57). Appellant submits that Dunn teaches away from using both passwords and portable cards because of their unreliability (see col. 1, lines 31-56).

Despite the fact the references clearly teach away from one another, the Examiner still contends that it would have been obvious for one skilled in the art to combine the teachings of Teicher with Moussa and Dunn because it would “provide another user input required to access the system, increasing security” and “by collating the PIN directly on the smart card, making it impossible...for another device ... to covertly obtain the PIN.” Final Office Action, paper 11, at page 5. In the Advisory Action of October 14, 2004 (paper 1), the Examiner contends that the teachings of Teicher can be logically combined with Moussa (See Advisory Action, paper no. 1 at pages 2-3).

“The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination.” MPEP at 2100-131 quoting *In re Mills*, 916 F.2d 680. Here, Appellant has clearly shown that Moussa, Teicher and Dunn teach away from one another for at least the reasons given above. Thus, the Examiner’s proffered reason that the teachings can be logically combined is not supported in the prior art.

The Examiner attempts to combine these references because it is the only way to show the claimed password, the claimed identification number and the claimed biological information as set forth in claim 1 in combination with the other features. However, in order to combine these references, the Examiner clearly ignores that the references teach methods of security that are in conflict, e.g., collating the PIN directly in the smart card as taught by Teicher is clearly in conflict with the non-interactive physical tokens as taught by Moussa.

Appellant submits that the only teaching that discloses that an identification number input can be logically combined with password and biological inputs is in Appellant's written description (See Specification at page 2, line 11 to page 3, line 23).

Thus, the Examiner's combination of the references can only be achieved by improper hindsight since it was with the aid of Appellant's own disclosure. Accordingly, Appellant submits that the Examiner has not made a *prima facie* case of obviousness.

In addition, Teicher discloses the use of an active physical token (energized smart card) (see Abstract). Teicher also discloses that it is necessary for a smart card reader to exchange data in order to verify that a smart card is genuine (See col. 7, lines 42-54).

Appellant submits that the transfer of data for this type of verification would require an execution of a program. Accordingly, a main principle of operation of Moussa would be undermined since Moussa teaches that executing a program without fully authenticating a user is not as secure as those systems which do. Since the combination of Teicher and Moussa would require a change to the principle of operation of the invention in Moussa, i.e., the execution of a program before fully authenticating a user; Appellant submits that the teachings of Teicher are not enough to render the claims *prima facie* obvious for at least this additional reason. See MPEP 2143.02 at page 2100-132.

Appellant submits that claims 3 and 7-10 are patentable at least by virtue of their dependency on claim 1.

Claim 5:

The Examiner has rejected claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Moussa in view of Dunn, Teicher and Pearson *et al.* (US 5,991,408 [“Pearson”]).

Appellant submits that the teachings of Pearson do not disclose or suggest at least the claimed collating the stored identification number with the identification number transmitted by the identification number input device on the claimed individual authentication card as set forth in claim 1, and the teachings of Pearson also do not make obvious the combination of Moussa, Teicher and Dunn. Therefore, because one skilled in the art would not have combined Moussa, Teicher and Dunn for at least the reasons stated above with respect to claim 1, Appellant submits that claim 5 is patentable at least by virtue of its dependency on claim 1.

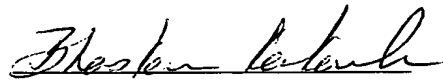
Appeal Brief
USSN 08/487,726

Attorney docket: Q57604
Art Unit 2131

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Bhaskar Kakarla
Registration No. 54,627

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: January 24, 2005

CLAIMS APPENDIX

CLAIMS 1, 3, 5, 7-10 ARE ON APPEAL:

1. An individual authentication system for authenticating the user of a data processing device storing a password, comprising:

an individual authentication card for storing biological information and a password for identifying a registered user;

a card reader for reading out the biological information and the password stored in the card;

a biological information input device for inputting biological information from a user; and

means for respectively collating the biological information and the password read from the card reader with the biological information from the biological information input device and the password stored in the data processing device,

wherein the data processing device has an identification number input device by which the user inputs an identification number; and

the card stores an identification number for identifying the registered user, and has a function of collating the stored identification number with the identification number transmitted by the identification number input device.

2. (canceled):

3. An individual authentication system as claimed in claim 1, wherein the biological information is fingerprint data.

4. (canceled):

5. An individual authentication system as claimed in claim 3, wherein the biological information is a plurality of fingerprint data.

6. (canceled):

7. An individual authentication system as claimed in claim 1, wherein the card is an IC card storing at least the biological information and the password for identifying a registered user as electric signals.

8. An individual authentication system as claimed in claim 1, wherein one or both of the biological information and the password are encrypted using an encrypting algorithm.

9. An individual authentication system as claimed in claim 1, wherein one or more of the biological information, the password, and the identification number are encrypted using an encrypting algorithm.

10. An individual authentication system as claimed in claim 1, wherein the card reader, the identification number input device, and the biological information input device are integrated in a single device.

Appeal Brief
USSN 08/487,726

Attorney docket: Q57604
Art Unit 2131

EVIDENCE APPENDIX:

NONE

Appeal Brief
USSN 08/487,726

Attorney docket: Q57604
Art Unit 2131

RELATED PROCEEDINGS APPENDIX

NONE